

# UD1\_T2 Integridad



Nicolás González Dobarro

# Índice

* WINDOWS - SFC *	3
- Ejecuta SFC en una máquina Windows 10 y muestra el resumen final.....	3
- Visualiza el log.....	3
* LINUX - Rootkit Hunter *	4
- Instala Rootkit Hunter en una máquina Ubuntu 14.....	4
- Actualiza Rootkit Hunter para que tenga en cuenta las aplicaciones y actualizaciones instaladas en tu S.O.....	4
- Ejecuta Rootkit Hunter y muestra el resumen final.....	5
- Visualiza el log, busca un archivo con Warnings y ábrelo con "gedit" para investigarlo.....	5

## \* WINDOWS - SFC \*

- Ejecuta SFC en una máquina Windows 10 y muestra el resumen final.

```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.

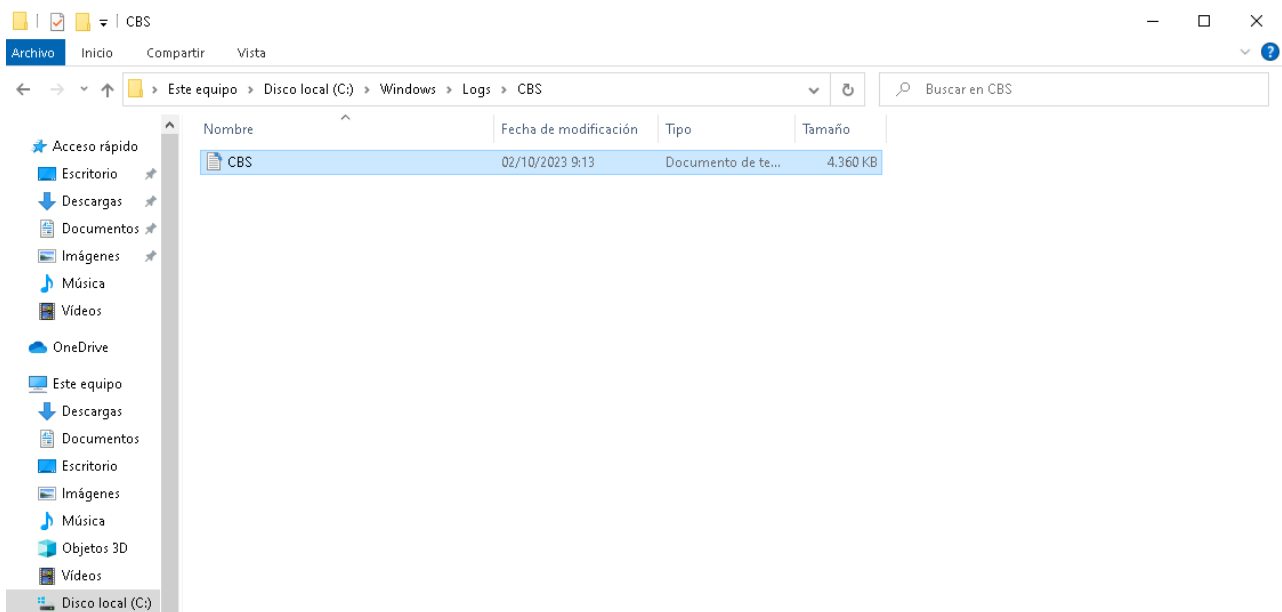
C:\Windows\system32>sfc /scannow

Iniciando examen en el sistema. Este proceso tardará algún tiempo.

Iniciando la fase de comprobación del examen del sistema.
Se completó la comprobación de 100%.

Protección de recursos de Windows encontró archivos dañados y los reparó correctamente.
Para las reparaciones en línea, los detalles se encuentran en el archivo de registro de CBS ubicado en
windir\Logs\CBS\CBS.log. Por ejemplo, C:\Windows\Logs\CBS\CBS.log. Para las reparaciones
sin conexión, los detalles se encuentran en el archivo de registro que proporciona la marca /OFFLOGFILE.
```

- Visualiza el log.



## \* LINUX - Rootkit Hunter \*

- Instala Rootkit Hunter en una máquina Ubuntu 14.

```
root@usuario:/home/usuario# aptitude install rkhunter
No se ha encontrado la orden «aptitude», pero se puede instalar con:
apt install aptitude
root@usuario:/home/usuario# apt install rkhunter
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
binutils binutils-common binutils-x86-64-linux-gnu bsd-mailx fonts-lato
javascript-common libbinutils libctf-nobfd0 libctf0 libjs-jquery
liblockfile-bin liblockfile1 libruby3.0 net-tools postfix rake ruby
ruby-net-telnet ruby-rubygems ruby-webrick ruby-xmlrpc ruby3.0
rubygems-integration unhide unhide.rb
Paquetes sugeridos:
binutils-doc apache2 | lighttpd | httpd procmail postfix-mysql postfix-pgsql
postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite sasl2-bin
| dovecot-common resolvconf postfix-cdb postfix-mta-sts-resolver postfix-doc
ri ruby-dev bundler
Se instalarán los siguientes paquetes NUEVOS:
binutils binutils-common binutils-x86-64-linux-gnu bsd-mailx fonts-lato
javascript-common libbinutils libctf-nobfd0 libctf0 libjs-jquery
liblockfile-bin liblockfile1 libruby3.0 net-tools postfix rake rkhunter ruby
ruby-net-telnet ruby-rubygems ruby-webrick ruby-xmlrpc ruby3.0
rubygems-integration unhide unhide.rb
0 actualizados, 26 nuevos se instalarán, 0 para eliminar y 5 no actualizados.
Se necesita descargar 13,8 MB de archivos.
Se utilizarán 59,1 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

- Actualiza Rootkit Hunter para que tenga en cuenta las aplicaciones y actualizaciones instaladas en tu S.O.

```
root@usuario:/home/usuario# apt update rkhunter
E: La orden de actualización no necesita argumentos
root@usuario:/home/usuario# apt upgrade rkhunter
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
rkhunter ya está en su versión más reciente (1.4.6-10).
Calculando la actualización... Hecho
Los siguientes paquetes se han retenido:
gir1.2-mutter-10 gjs libgjs0g libmutter-10-0 mutter-common
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 5 no actualizados.
root@usuario:/home/usuario#
```

- Ejecuta Rootkit Hunter y muestra el resumen final.

```
System checks summary
=====

File properties checks...
  Files checked: 142
  Suspect files: 1

Rootkit checks...
  Rootkits checked : 477
  Possible rootkits: 0

Applications checks...
  All checks skipped

The system checks took: 51 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

root@usuario:/home/usuario#
```

- Visualiza el log, busca un archivo con Warnings y ábrelo con "gedit" para investigarlo.

```
root@usuario:/home/usuario# cat /var/log/rkhunter.log
[08:41:17] Running Rootkit Hunter version 1.4.6 on usuario
[08:41:17]
[08:41:17] Info: Start date is mar 03 oct 2023 08:41:17 CEST
[08:41:17]
[08:41:17] Checking configuration file and command-line options...
[08:41:17] Info: Detected operating system is 'Linux'
[08:41:17] Info: Found O/S name: Ubuntu 22.04.3 LTS
[08:41:17] Info: Command line is /usr/bin/rkhunter --check
[08:41:17] Info: Environment shell is /bin/bash; rkhunter is using dash
[08:41:17] Info: Using configuration file '/etc/rkhunter.conf'
[08:41:17] Info: Installation directory is '/usr'
[08:41:17] Info: Using language 'en'
[08:41:17] Info: Using '/var/lib/rkhunter/db' as the database directory
[08:41:17] Info: Using '/usr/share/rkhunter/scripts' as the support script directory
[08:41:17] Info: Using '/usr/local/sbin /usr/local/bin /usr/sbin /usr/bin /sbin /bin
xec' as the command directories
[08:41:17] Info: Using '/var/lib/rkhunter/tmp' as the temporary directory
[08:41:17] Info: No mail-on-warning address configured
[08:41:17] Info: X will be automatically detected
[08:41:17] Info: Using second color set
```

```
lwp-request /usr/bin  
Abrir  Guardar  -  □  ×  
#!/usr/bin/perl  
2  
3 # Simple user agent using LWP library.  
4  
5 =head1 NAME  
6  
7 lwp-request - Simple command line user agent  
8  
9 =head1 SYNOPSIS  
10  
11 B<lwp-request> [B<-afPuUsSedvhx>] [B<-m> I<method>] [B<-b> I<base URL>] [B<-t> I<timeout>]  
12 [B<-i> I<if-modified-since>] [B<-c> I<content-type>]  
13 [B<-C> I<credentials>] [B<-p> I<proxy-url>] [B<-o> I<format>] I<url>...  
14  
15 =head1 DESCRIPTION  
16  
17 This program can be used to send requests to WWW servers and your  
18 local file system. The request content for POST and PUT  
19 methods is read from stdin. The content of the response is printed on  
20 stdout. Error messages are printed on stderr. The program returns a  
21 status value indicating the number of URLs that failed.  
22  
23 The options are:  
24  
25 =over 4  
26  
27 =item -m <method>  
28  
29 Set which method to use for the request. If this option is not used,  
30 then the method is derived from the name of the program.  
31  
32 =item -f  
33  
34 Force request through, even if the program believes that the method is  
35 illegal. The server might reject the request eventually.  
36  
37 =item -b <uri>  
38
```